



XIP1111B: AES128-GCM

Advanced Encryption Standard (128-bit key), Galois Counter Mode IP Core

Product Brief
ver. 1.0.1
February 27, 2020

sales@xiphera.com

Introduction

XIP1111B from Xiphera is a balanced Intellectual Property (IP) core implementing the Advanced Encryption Standard (AES) [2] in Galois Counter Mode (GCM) [3]. AES-GCM is a widely used cryptographic algorithm for Authenticated Encryption with Associated Data (AEAD) purposes, as it provides both data confidentiality and authenticity.

XIP1111B has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP1111B does not rely on any FPGA manufacturer-specific features.

Key Features

- **Compact** resource requirements: The entire XIP1111B requires less than 2800 Adaptive Lookup Modules (ALMs) (Intel® Cyclone®V), and does not require any multipliers, DSPBlocks or internal memory¹ in a typical FPGA implementation.
- **Performance:** Despite its compact size, XIP1111B achieves a throughput in the Gbps range², for example 2.5 Gbps in Xilinx® Artix®-7 family.
- **Standard Compliance:** XIP1111B is fully compliant with both the Advanced Encryption Algorithm (AES) standard [2], as well as with the Galois Counter Mode (GCM) standard [3].
- **Test Vector Compliance:** XIP1111B passes all test vectors specified in [1].

¹The parameterizable input and output FIFOs may optionally be instantiated with internal memory blocks, but the actual XIP1111B kernel requires only logic resources.

²As is typical for AEAD algorithms, the highest throughput is achieved for long messages.

- **32-bit FIFO Interfaces**³ ease the integration of XIP1111B with other FPGA logic and/or control software.

Functionality

The main functionality of XIP1111B depends on the mode of operation. When XIP1111B operates in the encryption and authentication tag calculation mode, it encrypts the incoming plaintext blocks into ciphertext blocks, and in addition to this also calculates a 128 bits long authentication tag from both the incoming plaintext and associated data. When XIP1111B operates in the decryption and tag validity checking mode, it decrypts the incoming ciphertext blocks into plaintext blocks, and validates the received authentication tag value by calculating the tag from the incoming ciphertext and associated data blocks and comparing the resulting tag value with the received tag value. As defined by the GCM mode of operation, associated data is included in the authentication tag calculation.

XIP1111B can also operate with zero-length associated data, meaning that XIP1111B treats all signals on the input `data_in` as plaintext to be encrypted or as ciphertext to be decrypted. XIP1111B can also operate with zero-length plaintext or ciphertext, in which case it acts only as an authenticator or authentication validity checker.

XIP1111B outputs first the associated data, followed by encrypted plaintext or decrypted ciphertext (depending on the mode of operation), and as the last output the tag value and associated status signals.

Block Diagram

The internal high-level block diagram of XIP1111B is depicted in Figure 1.

Interfaces

The external interfaces of XIP1111B are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP1111B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP1111B, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

FPGA Resources and Performance

Table 1 presents the FPGA resource requirements for representative implementations on two different FPGA architectures. On request, the resource estimates can also be supplied for other FPGA families.

Example Use Cases

Mention that XIP1111B is the balanced version, and XIP1211H is the high-speed version.

³XIP1111B is also available with 128-bits long interfaces, please contact sales@xiphera.com for details.

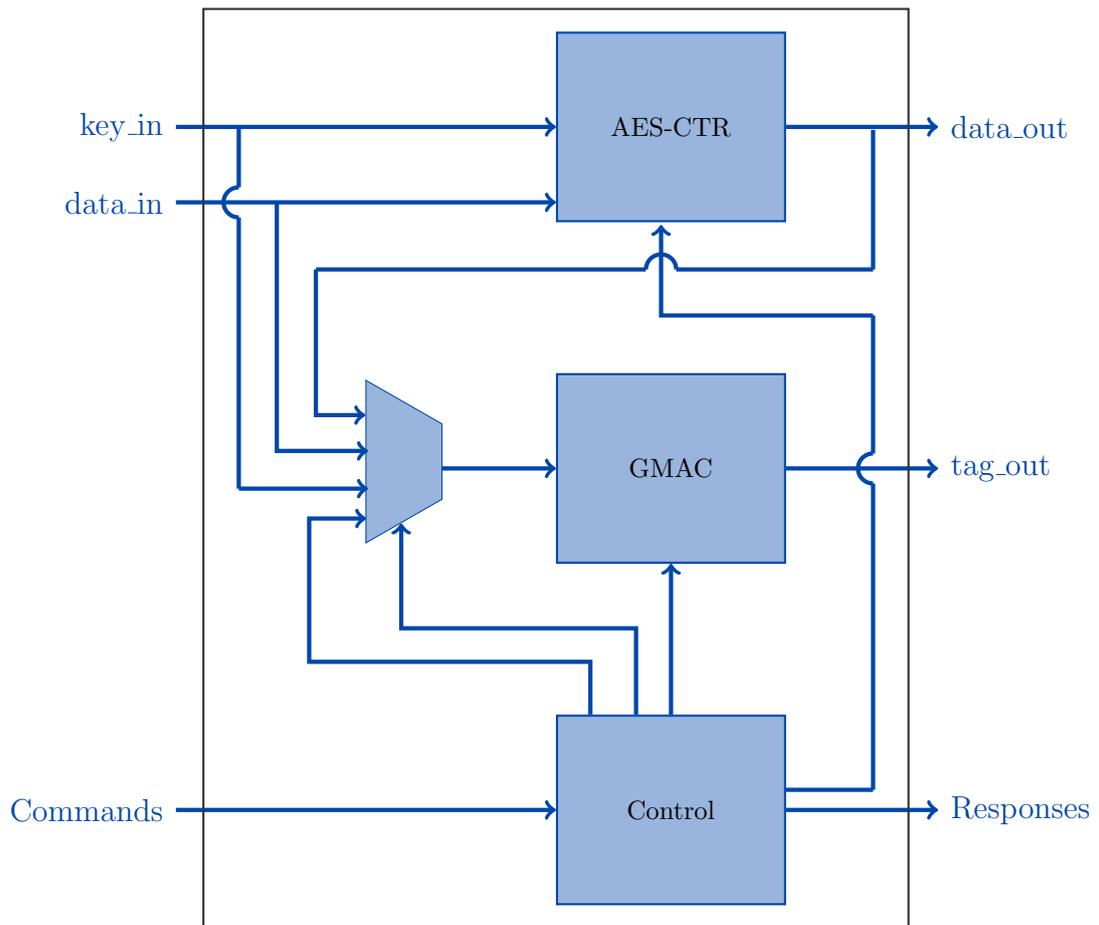


Figure 1: Internal high-level block diagram of XIP1111B

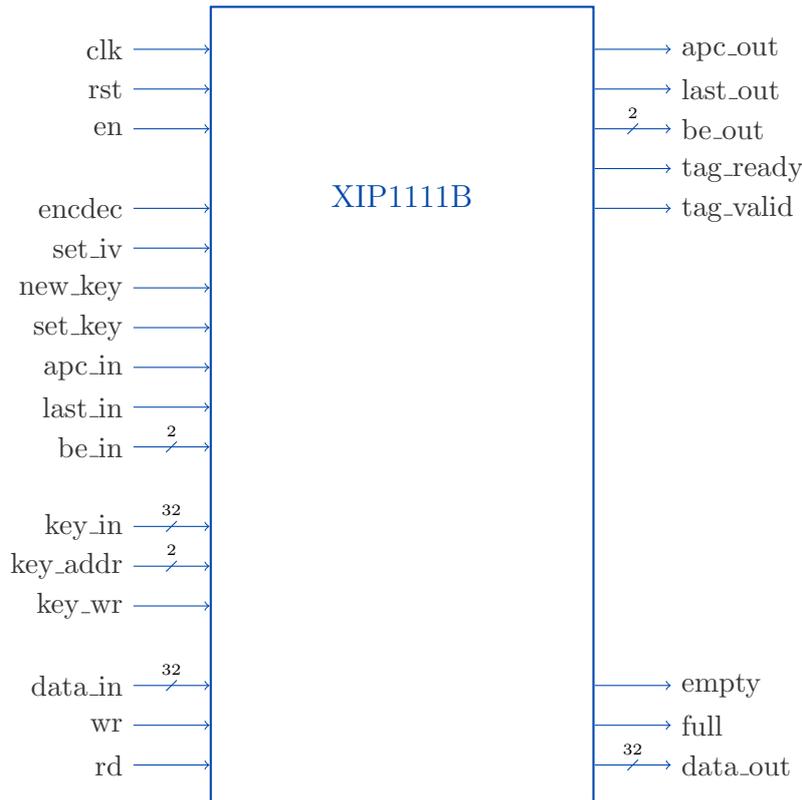


Figure 2: External interfaces of XIP1111B

Device	Resources	f_{MAX}	Max. throughput [‡]
Intel [®] Cyclone [®] V [†]	2797 ALM	130 MHz	1.5 Gbps
Xilinx [®] Artix [®] -7 [*]	2823 LUT, 5 BRAM FF	214 MHz	2.5 Gbps

[†] Quartus II Prime 19.1., default compilation settings, industrial speedgrade

^{*} Vivado 19.1., default compilation settings, industrial speedgrade

[‡] $Throughput = \frac{f_{MAX} * 128 \text{ bits}}{11 \text{ clock cycles}}$; achieved asymptotically with long packets.

Table 1: Resource usage and performance of XIP1111B on representative FPGA families.

Also mention that XIP1213B and XIP1213H are the 256-bit long key version.

Also mention that with certain boundary conditions being met XIP1111B can also be retrofitted to existing FPGA designs.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP1111B can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, a comprehensive VHDL testbench and a detailed datasheet are included.

Export Control

XIP1111B protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP1111B is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP1111B can be immediately shipped to all European Union member states, Australia, Canada, Japan, New Zealand, Norway, Switzerland, United Kingdom, and the United States.

Export to other countries requires authorization from The Ministry for Foreign Affairs of Finland, and a typical processing time for an export authorization is a few weeks.

About Xiphera

Xiphera specializes in secure and efficient implementations of standardized cryptographic algorithms on Field Programmable Gate Arrays (FPGAs). Our product portfolio includes individual cryptographic Intellectual Property (IP) cores, as well as comprehensive security solutions built from a combination of individual IP cores.

Xiphera is a Finnish company operating under the laws of the Republic of Finland, and is fully owned by Finnish citizens.

Contact

Xiphera Oy
Otakaari 5
FIN-02150 Espoo
Finland
sales@xiphera.com
+358 20 730 5252

References

- [1] MACsec GCM-AES Test Vectors. <http://www.ieee802.org/1/files/public/docs2011/bn-randall-test-vectors-0511-v1.pdf>.
- [2] Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001.
- [3] Morris J. Dworkin. SP 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. Technical report, Gaithersburg, MD, United States, 2007.